بسم الله الرحمن الرحيم

والحمد لله رب العالمين

والصلاة والسلام على سيدنا محمد النبي الكريم وعلى آله وأصحابه أجمعين

ربنا تقبل منا إنك أنت السميع العليم وتب علينا إنك أنت التواب الرحيم



يقول الله في كتابه العزيز

بسم الله الرحمن الرحيم

" وما أوتيتم من العلم إلا قليلا "

صدق الله العظيم

"رب أشرح لي صدري ويسر لي أمرى واحلل عقدة من لسانى يفقهوا قولي"

اللهم لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم

أخوكم في الله

م / مصطفى عبده توفيق محمد

جمهورية مصر العربية

كيف تفكر كالهاكر

Mostafa Digital

كيف تفكر كالهاكر

ستسمح لك دورة تدريبية في أمن المعلومات أن تنظر إلى شبكتك من خلال أعين المخترقين.

إن كنت مسؤولا عن أمن شبكتك، فعليك التعرف على عقلية المخترقين والأدوات التي يستخدمونها في هجماتهم.

فلا يكفي أن تركب أحدث برمجيات سد الثغرات الأمنية على المزودات ومحطات العمل لديك، أو أن يكون أسلوبك في الدفاع عن أمنك عبارة عن ردود أفعال. فإذا تعلمت ما يعلمه المخترقون، ستتاح لك فرصة أفضل للتعرف على نقاط الضعف لديك، وإزالتها، قبل وقوع الضرر. ويعتبر إتباع دورة تدريبية مكثفة حول المنهجية التي يتبعها المخترقون في اختبار نقاط ضعف الأنظمة للتمكن من التسلل إليها، إحدى أفضل وسائل التعلم.



قدمت لنا شركة Found Stone (www.foundstone.com)، وهي شركة تعمل في تطوير أدوات أمن المعلومات والتقييم الأمني، دعوة للانخراط في إحدى دوراتها التدريبية المسماة "دورة الاختراق الأقصى"، وهي دورة تضعك في بيئة المخترقين لمدة 4 أيام.

يأخذ برنامج Found Scan، وهو البرنامج الرئيسي لشركة FoundStone، منحىً مبتكراً في تحديد الثغرات الأمنية في الشبكات، ومساعدتك على سدها. لكن جدير بالذكر أن "دورة الاختراق الأقصى" ليست مجرد امتداد تجاري لتسويق منتجات وخدمات الشركة.

لا تعتبر هذه الدورة التدريبية، بأجورها التي تبلغ 3995 دولاراً، مناسبة لمن يشكل دافعهم الرئيسي الفضول فحسب. لكنها تستحق كل فلس يدفع مقابلها، بالنسبة للمسؤولين عن حماية شبكات معينة، كمديري الشبكات، ومديري تقنية المعلومات في الشركات.

يحصل كل تلميذ في هذه الدورة على حاسوب مفكرة، معد للإقلاع بشكل مزدوج (نظامي ويندوز 2000، ولينكس)، ومركب عليه مجموعة من معدات أمن المعلومات التي تنتجها الشركة، بالإضافة إلى عدد من أدوات الاختراق. ويتم تعلم استخدام هذه المنتجات والتدرب عليها من خلال تجارب مخبرية، تحاول فيها اختراق شبكات شركات جرت محاكاتها، في محاولة لسرقة معلوماتها.

قد يعتبر الاختراق جرماً يعاقب عليه قانونياً، لكنه يعتبر كذلك فرعاً من فروع المعرفة المعترف بها. وإليك في ما يلي بعضاً من الاستراتيجيات التي يستخدمها المخترقون عادة، والتي تشكل أساس الدورة التدريبية للشركة:

تحديد البصمات الرئيسية (foot printing):

هي عملية تجميع المعلومات الأساسية عن الهدف المقصود، خاصة عناوين النطاقات وعناوين IP. ويعتمد المخترقون على عدة خدع في عملية "تحديد البصمات الرئيسية"، بما في ذلك اللجوء إلى عديد من موارد المعلومات المتوفرة عبر إنترنت، مثل قواعد بيانات Whois، بالإضافة إلى محاولة تطبيق خطط تعتمد على ما يعرف بالهندسة الاجتماعية، التي يلجأ فيها المخترق إلى خداع مستخدمين ضمن الشبكة التي يحاول اختراقها بهدف دفعهم لإعطائه تلك المعلومات المهمة طوعاً. فيمكن مثلاً، أن يتصل المخترق بأحد مستخدمي الشبكة، منتحلاً شخصية موظف دعم فني، طالباً إعطاءه اسم الاستخدام وكلمة المرور، مدعياً أنه سيحتاجها لمعالجة مشكلة فنية في حساب هذا المستخدم.

مسح الشبكة (scanning):

يلجأ المخترقون إلى عملية مسح الشبكات في محاولة لإيجاد مزودات موصولة إلى الشبكة، أو غيرها من الجدران النارية أو الأجهزة الأخرى. ويستخدمون في هذه العملية أدوات مثل برنامج Nmap (www.insecure.org) الذي يبحث في الشبكات عن المنافذ المفتوحة والثغرات الأمنية.

الجرد (enumeration):

باستخدام هذه التقنية، يحاول المخترق التعرف على الحسابات المتوفرة على المزود المستهدف، أو تحديد الموارد التي جرى مشاركتها عبر الشبكة بطريقة ضعيفة أمنياً.

الاختراق (penetration):

يلجأ المخترق بهذه الطريقة إلى تخمين كلمات المرور إلى حسابات المستخدمين التي تعتمد كلمات مرور بسيطة.

التصعيد (escalation):

يحاول المخترق أن يرفع من مستوى الحقوق التي يملكها أحد الحسابات التي تمكّن من اختراقها، ليمنح هذا الحساب حقوقاً مماثلة لمدير الشبكة، وذلك باستخدام أدوات مثل PipeUpAdmin.

السلب (pillaging):

في عملية السلب، يحاول المخترق الحصول على ملفات كلمات المرور المشفرة (hashes)، محاولاً فك تشفيرها مستخدماً أدوات مثل L0phtCrack، أو John The Ripper، ثم تحميل برامج معينة إلى المزود، مثل الأدوات التي تسمح بالوصول إلى جذر نظام Unix لتسهيل محاولات الاختراق مستقبلاً.

تغطية الأثر (covering tracks):

ينشئ المخترقون عادة أبواباً خلفية أينما استطاعوا ذلك، لتتيح لهم الدخول إلى النظام لاحقاً. ويغطي المخترق آثاره ليمنع اكتشاف عملية الاختراق التي أجراها. وتصبح هذه الأجهزة المخترقة عادة، نقطة انطلاق للهجمات في المستقبل.

تمنحك المشاركة في هذه الدورة لأيام أربعة طاقة كبيرة، بحيث لن تشعر لاحقاً بأنك دائم التعرض للأخطار الكبيرة، كما لن تشعر بأنك آمن تماماً أو قادر على حماية شبكتك تماماً. وستمنحك التجارب التي تجريها في المختبر القدرة على التفكير من منظور أشمل خلال وقت قصير. فقد كان من الممتع جداً، التوصل خلال وقت قصير إلى حساب مدير شبكة أخرى، بتخمين كلمة مروره التي كانت بسيطة، حين كان جميع التلاميذ في الدورة يحاولون استخدام برنامج L0pht Crack لكسر كلمة المرور بحكم العادة! وتمكنوا بعد ذلك من اكتشاف مزود طرفي (Terminal) يعمل على الجهاز المستهدف، ثم استخدامه لتغيير جميع كلمات المرور ثم إطفاء الجهاز، ثم إضافة المزيد من الفوضى الحقيقية، من خلال منع مدربهم في الدورة من الوصول إلى ذلك الجهاز! علماً بأنهم اعترفوا لاحقاً بأنهم هم من فعل ذلك، وقدمت لائحة بكلمات السر الجديدة للمدرب. وقد شجع المدرب على هذا النوع من السلوك "ألاختراقي" للتعلم!

وإذا كنت لا تستطيع إقناع المدير المالي في شركتك أن حماية مقدرات الشركة جديرة بدفع 4000 دولار، فيمكنك أن تتخذ الخطوة الأولى بتعليم نفسك من خلال الكتاب الذي تعتمد عليه دورة شركة Found stone بشكل رئيسي، وهو: Hacking Exposed، من تأليف مدراء شركة Found stone ذاتهم، ستوارت مكلور، وجويل سكامبري، وجورج كرتز (السعر: 49.95 دولاراً من دار النشر McGraw-Hill).

كي تتمكن من اتخاذ رد الفعل المناسب ضد الأذكياء من المخترقين، عليك أن تتعلم كيف يفكرون، وأن تحاول تخمين ما ستكون خطواتهم التالية.

اخـــتراق الإنـــترنت

يبدو أن بعض المخترقين من ذوي النوايا الشريرة، يسعون إلى تدمير أكثر من مجرد مواقع إنترنت المستقلة. ونذكر هنا، المحاولة التي جرت في شهر أكتوبر/تشرين الأول الفائت، والتي حاول خلالها المخترقون إيقاف 13 مزود رئيسي لأسماء النطاقات (DNS) في إنترنت. صحيح أن الهجمات الموزعة لحجب الخدمة (DDoS) تلك، قد فشلت وقتها، إلا أنها تمكنت من إيقاف 7 مزودات DNS على الأقل. كما نذكر التهديد الذي شكله فيروس SQL Slammer نهاية شهر يناير/كانون الثاني الفائت، والذي هدد بقطع الوصول إلى إنترنت في أقاليم جغرافية كاملة.

اعتمد فيروس SQL Slammer على استغلال ثغرة أمنية شهيرة في إحدى خدمات مزودات قاعدة البيانات SQL التي تنتجها مايكروسوفت، علماً أن الرقعة الأمنية (patch) المطلوبة لسد هذه الثغرة متوفرة منذ مدة طويلة. لكن من المثير للسخرية، هو أن شركة مايكروسوفت ذاتها كان لديها عدداً من مزودات SQL التي لم يجر تركيب الرقعة الأمنية عليها، والتي تعرضت بدورها إلى هجمات فيروس SQL Slammer، ما شكل ضغطاً على شبكة مايكروسوفت ذاتها.

لم تتضح نية المهاجمين في تلك الهجمات، فهل كانوا يحاولون تدمير الوسط الرئيسي الذي يعتمدون عليه في عملهم، أم أنها مجرد محاولة لاختبار مهاراتهم؟! إلا أن الأمر الذي اتضح نتيجة تلك الهجمات هو أن الخطوات الأمنية الرئيسية لا يجري تطبيقها في أغلب الأحيان. على الرغم من صعوبة عملية سد الثغرات الأمنية في مزودات SQL، أو شبيهاتها من أنظمة التشغيل أو المزودات ذات المهمات الأساسية، إلا أنه لا مناص من إبقاء هذه المزودات محدثة بأحدث الرقع الأمنية، وإلا سيستمر المخترقون في تلقين مديري الأنظمة والشبكات الدروس الملائمة في أساسيات أمن المعلومات، وبتكاليف مرتفعة للغاية.



أرجو أن تكونوا استفدتم بقراءة هذا الكتاب ولتدعوا الله لي بظهر الغيب
ولأي استفسار بالرجاء مراسلتي على الرابط التالي :-

E mail :- MostafaDigital@yahoo!.com

ولكم تحياتي

م/ مصطفى عبده توفيق محمد